

ISSN 2095-7025
CN 10-1195/TN

密码学报

JOURNAL OF CRYPTOLOGIC RESEARCH

第1卷 第3期 Vol.1 No.3

2014年6月



主办



目 次

无线信道的密钥生成方法	李古月, 胡爱群, 石 乐 (211)
模背包向量问题的实际复杂度与基于格密码体制的实际安全性 彭力强, 胡 磊, 黄章杰, 许 军 (225)
EIGamal 加密方案的 KDM 安全性	常金勇, 薛 锐, 史 涛 (235)
RSA/Rabin-Paillier 陷门函数的比特安全性	康镇麒, 吕克伟 (244)
一类新的多项式型超 Bent 函数的刻画	唐春明, 亓延峰, 徐茂智 (255)
针对双线性对密码算法的分支故障攻击	丁兆晶, 姚晓旭, 魏继增, 顾海华, 郭 炜 (268)
一类完全非线性函数的构造及其唯一性	周子健, 周 悦, 李 超 (279)
构造 Feistel-SP 结构高阶差分区分器的新方法	董 乐, 吴文玲, 邹 剑, 杜 蛟, 李 锐 (287)
零相关线性分析研究	王美琴, 温 隆 (296)
中国密码学会 2014 年会通知	(234)
2014 年安全协议进展国际会议征稿启事	(243)
中国密码学会各专委会 2014 年 9-10 月主办学术会议一览	(310)
《密码学报》投稿指南	(封三)

CONTENTS

Secret Key Extraction in Wireless Channel	LI Gu-Yue, HU Ai-Qun, SHI Le (211)
Actual Complexity of Modular Knapsack Vector Problem and Practical Security of a Lattice Based Public Key Cryptosystem	PENG Li-Qiang, HU Lei, HUANG Zhang-Jie, XU Jun (225)
KDM Security of ElGamal Encryption Scheme	CHANG Jin-Yong, XUE Rui, SHI Tao (235)
On Bit Security of RSA/Rabin-Paillier Trapdoor Functions	KANG Zhen-Qi, LV Ke-Wei (244)
Characterization of a New Class of Hyper-Bent Functions in Polynomial Forms TANG Chun-Ming, QI Yan-Feng, XU Mao-Zhi (255)
Fault Attack on Branch of Pairing-based Cryptographic Algorithm DING Zhao-Jing, YAO Xiao-Xu, WEI Ji-Zeng, GU Hai-Hua, GUO Wei (268)
Construction and Uniqueness of a New Family of Perfect Nonlinear Functions ZHOU Zi-Jian, ZHOU Yue, LI Chao (279)
Novel Method of Constructing Higher-order Differential Distinguishers of Feistel-SP Structures DONG Le, WU Wen-Ling, ZOU Jian, DU Jiao, LI Rui (287)
Research on Zero-correlation Linear Cryptanalysis	WANG Mei-Qin, WEN Long (296)

密码学报

Mima Xuebao
(双月刊, 2014年创刊)
第1卷 第3期 2014年6月

Journal of Cryptologic Research (Bimonthly)

(Started in 2014)
Vol.1 No.3 Jun. 2014

编辑 《密码学报》编辑部
(北京市海淀区永翔北路9号 邮编100878)
电话: 86-10-81033105
传真: 86-10-81033101
E-mail: jcr@cacnet.org.cn
<http://www.jcr.cacnet.org.cn>

主编 裴定一

主办单位 中国密码学会 中国科学技术出版社

主管单位 中国科学技术协会

出版 中国科学技术出版社

印刷 北京科信印刷有限公司

发行 《密码学报》编辑部

Edited by Editorial Board of Journal of Cryptologic Research
(No. 9, North Yongxiang Road, Haidian District,
Beijing 100878, P. R. China)
Tel: 86-10-81033105
Fax: 86-10-81033101
E-mail: jcr@cacnet.org.cn
<http://www.jcr.cacnet.org.cn>

Editor-in-Chief PEI Ding-Yi

Sponsored by Chinese Association for Cryptologic
Research (CACR) and China Science and Technology Press
Supervised by China Association for Science and
Technology (CAST)

Published by China Science and Technology Press

Printed by Beijing Kexin Printing Co., Ltd.

ISSN 2095-7025
CN 10-1195/TN

公开发行

定价:60.00元